UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WISCONSIN

ROBERT PARK individually and on behalf of all others similarly situated, Plaintiff, v. AMERICAN FAMILY LIFE INSURANCE COMPANY and AMERICAN FAMILY MUTUAL INSURANCE COMPANY, S.I. Defendants.	Civil Action No. **COMPLAINT — CLASS ACTION** **JURY DEMAND**

Plaintiff Robert Park individually, and on behalf of all others similarly situated ("Plaintiff"), upon personal knowledge of facts pertaining to him and on information and belief as to all other matters, by and through undersigned counsel, hereby brings this Class Action Complaint against Defendants American Family Life Insurance Company and American Family Mutual Insurance Company, S.I. (collectively "American Family" or "Defendants"), and alleges as follows:

I. INTRODUCTION

1. Every year millions of Americans have their most valuable personal information stolen and sold online because of unauthorized data disclosures. Despite warnings about the severe impact of unauthorized data disclosures on Americans of all economic strata, companies—including Defendants—still fail to put adequate security

measures in place to prevent the unauthorized disclosure of private data belonging to their customers or potential customers.

2. American Family provides life insurance to customers across the country. American Family "recognize[s] the importance of our customers' trust. Keeping personal information confidential is a top priority."[1] American Family promises:

> Only authorized American Family Insurance workers, agents and their staff who need to know personal information while doing business are provided access. Their right to disclose or use this information is limited by our code of conduct, applicable law and non-disclosure agreements where appropriate. Individuals who violate our privacy policies are subject to disciplinary actions.[2]

3. Additionally, Defendants state that "[b]usinesses that collect personal information from consumers are required to have a security plan to protect the confidentiality and integrity of the information."[3]

4. Defendants provide online insurance quotes to consumers through their publicly accessible life insurance website. To make the quoting process easier for consumers, after a consumer enters basic personal information into the online quoting platform, American Family populates and displays additional personal information it has

---

[1] *Privacy Notice*, American Family Insurance, available at: https://www.amfam.com/privacy-security (last visited Feb. 10, 2022).

[2] *Id.*

[3] *Reducing Your Risk of a Data Breach*, American Family Insurance, available at: https://www.amfam.com/resources/articles/loss-control-resources/reduce-the-risk-of-a-data-breach (last visited Feb. 10, 2022).

in its possession and previously collected from other sources—such as driver's license numbers.[4]

5. American Family also provides online insurance quotes to consumers through its publicly accessible driver's insurance websites. These websites use the same quoting process as the American Family life insurance website described above.

6. Defendants failed to meet their promises and their obligation to protect the sensitive personal information they collected, maintained, and used—Defendants readily provided Plaintiff's and putative Class Members' driver's license number to *anyone* who entered a person's name and address into their online life insurance quoting platform. Thus, Defendants freely disclosed sensitive personal information belonging to customers, prospective customers, and even members of the general public who were not even prospective customers of Defendants, to the general public without consent and in violation of their own corporate promises and policy.

7. As reported by American Family on January 14, 2022, between December 5, 2021 and December 11, 2021, Defendants "believe unauthorized parties may have used an automated bot process" to access Plaintiff's "driver's license number as part of the platform's pre-fill function."[5] This means that for seven days, Plaintiff's and Class

---

[4] *See* Notice of Data Breach, Submitted Breach Notification Sample, California Attorney General, available at: https://oag.ca.gov/system/files/AFLIC%20Consumer%20letter%202022.01.14.pdf (last accessed Feb. 10, 2022); Notice of Data Breach, Data breach Notification Letters, Massachusetts Office of Consumer Affairs and Business Regulation, available at: https://www.mass.gov/doc/assigned-data-beach-number-25805-american-family-life-insurance-company/download (last accessed Feb. 11, 2022).

[5] *Id.*

Members' drivers' license numbers were essentially *publicly available* to anyone on Defendants' online life insurance quoting platform due to Defendants' negligent security practices and procedures.

8. While American Family has not yet reported the full extent of the unauthorized disclosures, it states there are approximately 306 affected individuals in Texas and Massachusetts alone.[6]

9. American Family is legally required to protect the personal information ("PI") they gather from unauthorized access and exfiltration. PI is defined as including a person's social security number, driver's license number, name, address, telephone number, and medical or disability information.[7]

10. American Family's failure to protect the driver's license information of Plaintiff and the Class on its life insurance website comes less than a year after it suffered an *identical breach* on its car insurance websites. Despite assurances in 2021 to individuals included in that data disclosure that it had made changes and eliminated the problem, the *same exact hacking attempt* using the *same exact methods* was successfully made on American Family's life insurance website.

[6] Massachusetts Data Breach Notification Report, Massachusetts Office of Consumer Affairs and Business Regulation , available at: https://www.mass.gov/doc/data-breach-report-2022/download (last accessed Feb. 11, 2022); Data Security Breach Reports, Attorney General of Texas, available at: https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last accessed Feb. 11, 2022).

[7] 18 U.S.C. § 2725(3).

11. As a result of Defendants' failure to provide reasonable and adequate data security, Defendants violated state and federal law by improperly disclosing Plaintiff's and the Class Members' PI—including their especially sensitive driver's license information—to unauthorized parties and/or entities. As a direct result of Defendants' acts and/or omissions, the unauthorized parties are already attempting to use the improperly disclosed information to commit identity theft and fraudulently open financial accounts in Plaintiff's name. And Plaintiff Park has *already* been the victim of identity theft. All Plaintiff and Class Members are now at much higher risk of continued identity theft and for cybercrimes of all kinds, especially considering the highly valuable and sought-after private PI stolen here, and have suffered damages related to lost time, loss of privacy, and other harms.

II. PARTIES

12. Plaintiff Robert Park is a resident of Alameda, California. On or about January 14, 2022, Plaintiff Park received notice from American Family that Defendants improperly exposed his PI to unauthorized third parties. Plaintiff Park never sought a quote of any sort from American Family.

13. Defendant American Family Life Insurance Company is a privately held insurance company incorporated in Wisconsin and headquartered in Madison, Wisconsin. American Family is licensed to do business and markets and sells insurance policies in Arizona, Colorado, California, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Michigan, Minnesota, Missouri, North Carolina, Nebraska, Nevada, North Dakota, Ohio, Oregon, South Carolina, South Dakota, Texas, Utah, Virginia, Washington, and Wisconsin.

14. Defendant American Family Mutual Insurance Company, S.I. is a privately held mutual insurance company incorporated in Wisconsin and headquartered in Madison, Wisconsin. American Family is licensed to do business and markets and sells insurance policies in Arizona, Colorado, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Minnesota, Missouri, Nebraska, Nevada, North Dakota, Ohio, Oregon, South Dakota, Utah, Washington, and Wisconsin.

III. JURISDICTION AND VENUE

15. Subject matter jurisdiction in this civil action is authorized pursuant to 28 U.S.C. § 1332(d) because there are more than 100 Class Members, at least one class member is a citizen of a state different from that of Defendants, and the amount in controversy exceeds $5 million, exclusive of interest and costs. The Court also has federal question jurisdiction under 28 U.S.C. § 1331 for the Drivers' Privacy Protection Act claims and supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

16. This Court has personal jurisdiction over Defendants because they maintain their principal place of business in this District, are registered to conduct business in Wisconsin, and have sufficient minimum contacts with Wisconsin.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendants reside in this District and, on information and belief, a substantial part of the events or omissions giving rise to Plaintiff's and Class Members' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Defendants Collect PI and Failed to Adhere to Non-Disclosure Requirements.

18. American Family has sold insurance since 1927 under various named and corporate forms. "The American Family Enterprise is a family of companies dedicated to delivering unparalleled service and exceptional protection to our customers."[8] Through its family of companies, it offers various types of insurance policies, including vehicle, home, life, renters' and business.[9]

19. Like other insurance providers, American Family has an online quote platform available to all persons capable of accessing it via the internet. Visitors to American Family insurance websites can "Get A Quote" instantly after providing some personal information. The same insurance online quote platform is available for American Family's life and auto insurance products.

20. Defendants' quoting feature uses the information entered by the website's visitor, combines it with additional information Defendants have, and then automatically displays the additional information to the visitor as part of the quote process.

21. Specifically, Defendants' quoting feature, which is still available on their website, asks a potential customer for a name, date of birth, and then an address. Once that information is entered, Defendants' system auto-populates the quotation with driver's license information from their own databases or from third-party prefill services and makes

[8] Our Story, American Family Insurance, available at: https://www.amfam.com/about/our-story (last accessed Feb. 11, 2022).

[9] https://www.amfam.com/insurance (last accessed Feb. 11, 2022);

that information visible to the person entering the information on the American Family quote website.

22. Defendants' online quote website did not require verification that the person or automated process entering name, date of birth, and address information was the same person for whom the information was being entered. Instead, and unfortunately, Defendants' online quote system was configured to provide PI—such as driver's license numbers—about anyone from their system by just entering a person's name and address. Thus, Defendants' online quoting platform allowed any site visitor to access and view PI of anyone Defendants had collected PI about.

23. Defendants believe an automated process, or "bot," was used on the instant quote feature to obtain Plaintiff's and Class Members drivers' license numbers, which includes many people who never applied for insurance with Defendants or were even necessarily aware of Defendants' existence. In other words, Defendants believe an unauthorized party availed themselves of the PI Defendants made publicly available via their instant quote feature.

24. This incident is referred to herein as the "Unauthorized Data Disclosure."

25. Plaintiff Park, along with members of the Class, received a letter from American Family titled "Notice of Data Breach," dated January 14, 2022. The letter stated that their PI, detailed below, may have been compromised, and included the following:

> **What Happened**
> We believe unauthorized parties may have used an automated bot process to enter certain personal information (such as your name and address) from unknown sources into the AFLIC online quoting platform. By doing so, they

may have accessed your driver's license number as part of the platform's pre-fill function.

We are notifying you because you may have been affected by this incident. If you did not request an online insurance quote using the AFLIC quoting platform between December 5, 2021 and December 11, 2021, the unauthorized parties may have requested a quote in your name and may have obtained your driver's license number. If, however, you did request an online quote from the American Family Life Insurance quoting platform between December 5, 2021 and December 11, 2021, you are not impacted by this incident.

What Information Was Involved
To the extent you were affected by this incident, unauthorized parties may have obtained your driver's license number.

We have reason to believe this data could be used to fraudulently apply for unemployment benefits in your name. Please carefully review any written communications you receive from your state's unemployment agency, especially if you have not applied for unemployment benefits. If you suspect that your data has been used to fraudulently apply for unemployment benefits, you should contact the relevant state unemployment agency immediately.

What We Are Doing
We identified the unauthorized activity and immediately took action to address it. We blocked the activity and worked to notify potentially affected consumers. If you did not previously have a relationship with AFLIC, we will delete your information once our investigation is complete and we have met our legal and regulatory obligations.

We take our responsibility to safeguard personal information seriously and we have enhanced our security controls to help prevent this type of incident from reoccurring.

To further help protect you, we are offering you **Single Bureau Credit Monitoring*** services free of charge. These services from Sontiq, through Identity Force, a TransUnion company, an independent outside firm, will provide you with alerts for 12 months from the date of enrollment whenever changes occur to your TransUnion credit file. The alert is sent to you the same day that the change or update takes place with the credit bureau. To enroll in these services, please log on to https://secure.identityforce.com/benefit/amfam and follow the online

instructions. Representatives are not able to process enrollments. They can only provide guidance. When prompted, please provide the following unique code to receive services:

Important *– You must register your account and activate your monitoring services within 90 days from the date of this letter, otherwise your ability to access the services will expire.*

There was no delay in providing you this notification as a result of a law enforcement investigation.

What You Can Do
It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. If you wish to monitor your own credit report for unauthorized activity, you may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies: TransUnion, Equifax and Experian. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at (877) 322-8228.

Additional information on identify theft protection is also provided in the enclosed pages entitled "Information About Identity Theft Protection."

For More Information
We take the security and privacy of your information very seriously and apologize for any inconvenience this incident may have caused. If you have any questions or concerns regarding this matter, please contact Sontiq at 1-888-514-2103 between 8 a.m. and 8 p.m. Eastern time, Monday through Friday. Representatives are available for 90 days.

Sincerely,

Chris Szafranski
Privacy Director
American Family Life Insurance Company, a subsidiary of American Family Mutual Insurance Company, S.I. privacyincident@amfam.com.[10]

[10] *Notice of Data Breach*, as filed with the California Attorney General, https://oag.ca.gov/system/files/AFLIC%20Consumer%20letter%202022.01.14.pdf (last accessed on Feb. 15, 2022).

26. The Notice confirms Plaintiff was a victim of the Unauthorized Data Disclosure even though he did not have a prior relationship with Defendant. Indeed, the Notice advised that Plaintiff was affected *only* if he *had not* sought an insurance quote from Defendant.

27. The Notice also confirms that driver's license numbers were acquired. And the Notice confirms that the hackers already had PI about Plaintiff and Class Members and used the Defendants' website to obtain and link additional PI, including driver's license numbers and addresses, in noting that Defendants "believe unauthorized parties may have used an automated bot process to enter certain personal information (such as your name and address) from unknown sources."

28. After receiving Unauthorized Data Disclosure notice letters, it is reasonable for Plaintiff and Class Members in this case to believe that the risk of future harm (including identity theft) is substantial and imminent, and to take steps to mitigate that substantial risk of future harm. In fact, Defendants' letter acknowledges the harm related to potential fraudulent use of the data—including providing a warning of a specific danger regarding unemployment benefits—and Defendants encourage affected individuals to use the identity theft protection service offered and note that "It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity."[11] This is because the drivers'

[11] *Id.*

license numbers are taken for the purpose of committing fraud in the name of the person whose license information is taken.

B. The PI Disclosed by Defendants as a Result of Their Disregard for Data Security is Highly Valuable on the Black Market.

29. The information Defendants voluntarily disclosed via their online quoting system in violation of state and federal law is very valuable to phishers, hackers, identity thieves, and cyber criminals, especially at this time where unprecedented numbers of criminals are filing fraudulent unemployment benefit claims and driver's license information is uniquely connected to the ability to file a fraudulent unemployment benefit claim and other financial fraud.

30. Indeed, these hackers often aggregate information taken from these breaches on users to build profiles on individuals. These profiles combine publicly available information with information discovered in previous data breaches and exploited vulnerabilities. There are few data breaches that provide a comprehensive snapshot of any one individual person. Unique and persistent identifiers such as Social Security Numbers, driver's license numbers, usernames, and financial account numbers (e.g., credit cards, insurance policy numbers, etc.) are critical to easily forging an identity. When not all information is available, the information that is stolen is used to socially engineer a victim into providing additional information so a "fullz"[12] profile can be obtained.

31. For example, a health care system and a retail store point-of-sale system may have two unrelated data breaches where an individual's information is taken. The

[12] "Fullz" is slang used by threat actors and various criminals meaning "full information," a complete identity profile or set of information on any entity or individual.

individual's driver's license may not be in either of those data bases, but after the Unauthorized Data Disclosure, a threat actor could have improved the profile and added a driver's license number. The value of that profile would allow such crimes as identity theft, financial crimes, and even illegal voting that would not previously have been possible.

32. There is no legitimate or legal reason for anyone to use Defendants' inadequate website security to acquire driver's license information Plaintiff and the Class. The only reason is for immediate or eventual malicious intent, since no one would go to the trouble of obtaining data that had no value. Any non-public data, especially government issued identification numbers like a driver's license or non-driver's identification number, has criminal value. On the darknet markets, a driver's license, combined with the full name and state issued, is a sought-after data point. Darknet markets are a downstream "flea market" for data to be sold, usually not by the original threat actor or criminal group. It is a dumping ground, usually after the data has been exploited.

33. The value of stolen driver's license information currently has a darknet market (DNM) value of $1 per license. This was re-verified on March 3, 2022, accessing several DNM using a trusted identity. Social Security Numbers, once considered the "gold standard" of identity fraud, are also selling for $1 per value in those same markets. This illustrates the value of driver's license information to cybercriminals and people committing identity fraud. According to popular darknet markets, cyber criminals value driver's licenses equally to Social Security Numbers.

34. In some ways, driver's license numbers are even more attractive than Social Security Numbers to threat actors and more dangerous to the consumer when

compromised. Unlike a Social Security Number, a driver's license number isn't monitored as closely, so it can potentially be used in ways that won't immediately alert the victim. Threat actors know this as well. Because driver's licenses contain, or can be used to gain access to, uniquely qualifying and comprehensive identifying information such as eye color, height, weight, sex, home address, medical or visual restrictions, and living will/health care directives, most insurance and credit agencies highly recommend that immediate notice, replacement, and identity theft protections are put in place for a minimum of 3 years. Most cyber experts, including Enterprise Knowledge Partners, recommend five years or more.

35. Stolen driver's licenses can be used (alone or in combination with other information) by malicious actors to accomplish the following:

- Apply for credit cards
- Apply for financial loans (especially student loans)
- Open bank accounts
- Obtain or create fake driver's licenses
- Given to police for tickets
- Provided to accident victims
- Collect government unemployment benefits
- Create and sell underage fake IDs
- Replace/access account information on:
    - LinkedIn

- Facebook/Meta
- WhatsApp
- Instagram

- Obtain a mobile phone
- Dispute or prove a SIM swap
- Redirect U.S. mail
- Apply for unemployment benefits
- Undocumented aliens may use them as a method to gain access to the U.S., and claim a lost or stolen passport
- Create a fake license as a baseline to obtain a Commercial Driver's License
- File tax returns or gain access to filed tax returns
- Engage in phishing and other social engineering scams

36. The process that was used to extract the data from Defendants' website based on their flaws and lack of security was likely automated. The Notice confirms this when it notes that "We believe unauthorized parties may have used an automated bot process to enter certain personal information (such as your name and address) from unknown sources into the AFLIC online quoting platform. By doing so, they may have accessed your driver's license number as part of the platform's pre-fill function."

37. Unsecured sites that contain or transmit PI, such as a driver's license, require notice to consumers when the data is stolen because it can be used to perform identity theft and other types of fraud. A threat actor is usually motivated by financial or political gain

before it exerts time, and skill to compromise and exfiltrate. Over time, identity thieves have systematized their criminal activities to gather important pieces of a synthetic identity from multiple breaches and sources. The theft of a driver's license number is no less valuable in that endeavor than the theft of a Social Security Number, as demonstrated by these two unique identifiers carrying the same price on the darknet, and by the fact that the identity thieves have demonstrated a systematic and businesslike process for collecting these stolen driver's license numbers in this Unauthorized Data Disclosure and others committed against insurers.

38. The frequency of cyberattacks has increased significantly in recent years.[13] In fact, "Cyberattacks rank as the fastest growing crime in the US, causing catastrophic business disruption. Globally, cybercrime damages are expected to reach US $6 trillion by 2021."[14]

39. Cybersecurity Ventures, a leading researcher on cybersecurity issues,

> expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, is exponentially larger than the damage inflicted from natural disasters in a

[13] *See The Cost of Cybercrime*, Accenture Security, available at: https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf (last accessed Feb. 15, 2022).

[14] *Top Cyberattacks of 2020 and How to Build Cyberresiliency*, ISAC, available at: https://www.isaca.org/resources/news-and-trends/industry-news/2020/top-cyberattacks-of-2020-and-how-to-build-cyberresiliency (last accessed Feb. 15, 2022) (citing Cybersecurity Ventures, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016).

> year, and will be more profitable than the global trade of all major illegal drugs combined.[15]

40. As noted in recent reports by Deloitte and Interpol, cyberattacks have greatly increased in the wake of the COVID-19 pandemic.[16]

41. As alleged above, stolen PI is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

42. When malicious actors infiltrate companies and exfiltrate the PI that those companies store or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[17] "Why else would hackers . . . steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015),

---

[15] Steve Morgan, *Cybercrime To Cost The World $10.5 Trillion Annually By 2020*, Cybercrime Magazine, Nov. 13, 2020, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (last accessed Feb. 15, 2022).

[16] Deloitte, *Impact of COVID-19 on Cybersecurity*, https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html (last accessed Feb. 15, 2022); Interpol, *Cyberthreats are constantly evolving in order to take advantage of online behaviour and trends. The COVID-19 outbreak is no exception*, https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats (last accessed Feb. 15, 2022).

[17] *Shining a Light on the Dark Web with Identity Monitoring*, IdentityForce, Dec. 28, 2020, *available at:* https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Feb. 15, 2022).

43. For example, when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay,

> are awash with [PI] belonging to victims from countries all over the world. One of the key challenges of protecting PI online is its pervasiveness. As unauthorized data disclosures in the news continue to show, PI about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target.[18]

44. Consumers' PI remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[19]. Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[20] Alternatively,

[18] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, *available at:* https://www.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited Feb. 15, 2022).

[19] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Feb. 15, 2022).

[20] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Feb. 15, 2022).

criminals are able to purchase access to entire company data breaches for $900 to $4,500.[21] (Note: the prices can vary depending on the point in the chain – verified identities may sell for higher prices early in the chain, then for the lower prices described above when they reach the "flea market sites.")

45. The information compromised in the Unauthorized Data Disclosure is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. And the information compromised in the Unauthorized Data Disclosure can be used to *open* fraudulent bank accounts and credit and debit cards, compounding the identity theft and cycle of black market sales detailed above. The driver's license numbers compromised in this Unauthorized Data Disclosure is also more valuable because driver's license numbers are long lasting, and difficult and problematic to change.

46. Recently, Forbes writer Lee Mathews reported on Geico's unauthorized data disclosure that included driver's license numbers:

> Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200.[22]

---

[21] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Feb. 15, 2022).

[22] Lee Mathews, *Hackers Stole Customers' License Numbers from Geico in Months-Long Breach*, (April 20, 2021), *available at*: https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3066c2218658 (last visited Feb. 15, 2022).

47. National credit reporting company, Experian, blogger Gayle Sato also emphasized the value of driver's license information to thieves and cautioned:

> Your driver's license may not seem like a jackpot for thieves, but it can be used to create fake driver's licenses, open accounts in your name, avoid traffic tickets or collect government benefits such as unemployment checks. Worse, if your license data has been stolen in a data breach, you may not even know it's being misused.[23]

48. In fact, according to CPO Magazine, which specializes in news, insights and resources for data protection, privacy and cyber security professionals,

> To those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation. Tim Sadler, CEO of email security firm Tessian, points out why this is not the case and why these numbers are very much sought after by cyber criminals: " . . . It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks. . . . bad actors may be using these driver's license numbers to fraudulently apply for unemployment benefits in someone else's name, a scam proving especially lucrative for hackers as unemployment numbers continue to soar. . . . In other cases, a scam using these driver's license numbers could look like an email that impersonates the DMV, requesting the person verify their driver's license number, car registration or insurance information, and then inserting a malicious link or attachment into the email.[24]

---

[23] Gayle Sato, *What Should I Do If My Driver's License Number Is Stolen?* (Nov. 3, 2021), *available at*: https://www.experian.com/blogs/ask-experian/what-should-i-do-if-my-drivers-license-number-is-stolen/ (last visited Feb. 15, 2022).

[24] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, (April 23, 2021), available at: https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-

49. Drivers' license numbers have been taken from auto-insurance providers by hackers in other circumstances, including Geico and Farmers both in 2021, indicating both that this particular form of PI is in high demand[25] and also that Defendants knew or had reason to know that their security practices were of particular importance to safeguard consumer data.[26] And *indeed,* American Family suffered this *exact same breach* on its auto insurance website in 2021, meaning it not only had general notice that this kind of information was valuable and in need of protection, but also specific notice of vulnerabilities *in Defendants' system.*

50. In fact, when Geico announced that its online quoting platform—which is nearly identical to Defendants'—was subject to a near-identical breach, its data breach notice filed with the California Attorney General explicitly stated that GEICO had "reason to believe that this information could be used to fraudulently apply for unemployment benefits in your name."[27]

---

numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed Feb. 14, 2022).

[25] *Id.*

[26] *See* United States Securities and Exchange Commission Form 8-K for INSU Acquisition Corp. II (Feb. 1, 2021), available at: https://www.sec.gov/Archives/edgar/data/1819035/000121390021005784/ea134248-8k_insuacquis2.htm?=1819035-01022021 (last accessed Feb. 15, 2022) (announcing a merger with auto-insurance company MetroMile, Inc., an auto-insurer, which announced a drivers' license number Data Disclosure on January 19, 2021); Ron Lieber, *How Identity Thieves Took My Wife for a Ride*, N.Y. TIMES (Apr. 27, 2021), available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed Feb. 15, 2022) (describing a scam involving drivers' license numbers and Progressive Insurance).

[27] *See https://www.documentcloud.org/documents/20618953-geico-data-breach-notice* (GEICO notice filed with Cailfornia Attorney General dated April 9, 2021)

51. Further, an article on TechCrunch explains that it is driver's license or non-driver's identification numbers themselves that are the critical missing link for a fraudulent unemployment benefits application: "Many financially driven criminals target government agencies using stolen identities or data. But many U.S. states require a government ID — like a driver's license — to file for unemployment benefits. To get a driver's license number, fraudsters take public or previously breached data and exploit weaknesses in auto insurance websites to obtain a customer's driver's license number. That allows the fraudsters to obtain unemployment benefits in another person's name."[28]

52. For example, the New York State Department of Financial Services issued an industry letter on February 16, 2021, stating that they had "recently learned of a systemic and aggressive campaign to exploit cybersecurity flaws in public-facing websites to steal [NPI, including] websites that provide an instant quote. . . . [I]t received reports from two auto insurers in late December 2020 and early January 2021, that cybercriminals were targeting their websites that offer instant [] quotes [] to seal unredacted driver's license numbers. . . . . DFS has confirmed that, at least in some cases, this stolen information has been used to submit fraudulent claims for pandemic and unemployment benefits."[29]

---

[28] Zach Whittaker, *Geico Admits Fraudsters Stole Customers' Driver's License Numbers for Months*, TechCrunch (Apr. 19, 2021), https://techcrunch.com/2021/04/19/geico-driver-license-numbers-scraped/#:~:text=To%20get%20a%20driver's%20license,benefits%20in%20another%20person's%20name (last accessed Mar. 2, 2022).

[29] https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert (last accessed March 7, 2022).

53. Once PI is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details, or to fraudulently manufacture new accounts for access and sale. This can lead to additional PI being harvested from the victim, as well as PI from family, friends and colleagues of the original victim.

54. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.[30]

55. Victims of drivers' license number theft also often suffer unemployment benefit fraud, harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts. Unauthorized data disclosures facilitate identity theft as hackers obtain consumers' PI and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PI to others who do the same.

56. Unauthorized data disclosures facilitate identity theft as hackers obtain consumers' PI and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PI to others who do the same.

[30] FBI, *2019 Internet Crime Report Released, Data Reflects an Evolving Threat and the Importance of Reporting* (Feb. 11, 2020), *available at*: https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed Feb. 15, 2022).

57. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use PI to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[31] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[32]

C. Defendants Were on Notice of the Sensitive and Private Nature of the PI It Stored and Utilized for Insurance Quotes, and Their Duty to Safeguard the PI.

58. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PI and of the foreseeable consequences if their data security systems were breached, including the significant costs that would be imposed on Plaintiff and the Class as a result of a breach.

59. "Insurance companies are desirable targets for cyber attackers because they work with sensitive data."[33] In fact, according to the Verizon 2020 Data Breach

[31] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), available at http://www.gao.gov/assets/270/262899.pdf (last visited May 29, 2021).

[32] *Id.*

[33] Data Protection Compliance for the Insurance Industry (October 7, 2020), *available at*: https://www.ekransystem.com/en/blog/data-protection-compliance-insurance-industry (last visited Feb. 15, 2022).

Investigations Report, there were 448 confirmed data breaches in the financial and insurance industries.[34]

60. Defendants claim:

> We maintain the integrity of information collected and consider privacy in the design of our systems, applications, products, and services, including implementing physical, electronic and administrative controls to safeguard your personal information[.] . . .
>
> Only authorized American Family Insurance workers, agents and their staff who need to know personal information while doing business are provided access. Their right to disclose or use this information is limited by our code of conduct, applicable law and non-disclosure agreements where appropriate.[35]

61. In addition, American Family is an insurance company that sells auto insurance and uses motor vehicle records to verify identities and underwrite policies. Their underwriting and other insurance activities are explicitly subject to the DPPA, which was enacted in 1994 and has been in effect for almost two decades.

62. In addition, Defendants consciously use PI and information about customers on an ongoing basis. Defendants' continual collection of PI in the form of customer information, driving records, accident reports, and other motor vehicle information, along with their insurance underwriting and business collection of driver's license and other motor vehicle information, put American Family in the position of knowing that it was

[34] 2020 Data Breach Investigations Report, Verizon, available at: https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf (last visited Feb. 15, 2022).

[35] Privacy and Security, American Family Insurance, https://www.amfam.com/privacy-security (last visited Feb. 15, 2022).

obligated to protect the privacy of customers and potential customers like Plaintiff and members of the class.

63. Most egregiously, American Family was specifically on notice of the manner and mechanism of the Unauthorized Data Disclosure because American Family *notified 283,734 people* in *May 2021* that an *identical data disclosure* occurred on its auto insurance website. Specifically, American Family's May 2021 notice, as provided to the Maine Attorney General, states:

> We are writing to inform you of a recent data security incident involving an online auto insurance quoting platform of American Family Mutual Insurance Company, S.I. (American Family). You may have been affected by an unauthorized attempt to obtain your personal data through this quoting platform.
>
> This letter will provide you with information about the incident and a no-cost service that American Family is making available to you to help monitor potential misuse of your personal data.
>
> **What Happened**
> We believe unauthorized parties may have used an automated bot process to obtain your driver's license number by entering personal information (such as your name and address) they acquired from unknown sources into the American Family quoting platform.
>
> We are notifying you because you may have been affected by this incident. If you did not request an insurance quote using the American Family quoting platform between February 6, 2021 and March 19, 2021, the unauthorized parties may have requested a quote in your name and may have obtained your driver's license number. If, however, you did request a quote from the American Family quoting platform between February 6, 2021 and March 19, 2021, you are not impacted by this incident.
> **What Information Was Involved**
> To the extent you were affected by this incident, unauthorized parties may have obtained your driver's license number.
>
> We have reason to believe this data may be used to fraudulently apply for unemployment benefits in your name. Please carefully review any written

> communications you receive from your state's unemployment agency, especially if you have not applied for unemployment benefits. If you suspect that your data has been used to fraudulently apply for unemployment benefits, you should contact the relevant state unemployment agency immediately.[36]

64. American Family knew that its online quoting platforms were vulnerable to hackers, not adequately secured, and that driver's license information could be stolen. And in fact, American Family has admitted as such when asked by Plaintiff Park. On February 2, 2022, Hannah Wilson, a privacy consultant with American Family Insurance, called Mr. Park to discuss the Unauthorized Data Disclosure. During their conversation, Plaintiff Park asked Ms. Wilson why the pre-fill function was not corrected after the first data breach in March of 2021. Ms. Wilson was very apologetic and said that American Family experienced a divisional breakdown between the insurance division and the corporate division, and told Plaintiff Park that the corporate side did not communicate the cause of the problem to the insurance division and the issue was not fixed. Ms. Wilson also explained that credit monitoring will not prevent the fraudulent filing of unemployment benefits, nor is there any way to do so.

65. As a result, American Family's safety and security promises were facially insufficient. Defendants' negligently designed online quoting system allowed access to and disclosure of Plaintiff's and Class Members' driver's license numbers in violation of Defendants' company policy, and applicable law.

---

[36] American Family Mutual Insurance Company, S.I.'s *Notice of Data Breach*, as filed with the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/b6f6658b-5592-4438-bac0-3280190754f3.shtml (last accessed on March 24, 2022).

D. Defendants Failed to Comply with Federal Trade Commission Requirements.

66. Federal and state governments established security standards and issued recommendations to minimize unauthorized data disclosures, and the resulting harm to individuals and financial institutions. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[37]

67. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[38] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[39]

---

[37] Federal Trade Commission, *Start With Security: A Guide for Business*, available at: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Feb. 15, 2022).

[38] *See* Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 15, 2022).

[39] *Id.*

68. Also, the FTC recommends companies limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify third-party service providers have implemented reasonable security measures.[40]

69. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect PI, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[41]

70. Through negligence in designing and implementing their online quoting platform and securing Plaintiff's and Class Members' PI, Defendants allowed the general public—and thieves—to utilize their online instant quote platform to obtain access to and collect individuals' PI. Defendants failed to employ reasonable and appropriate measures to protect against unauthorized disclosure and access to Plaintiff's and Class Members' PI. Defendants' data security policies and practices constitute unfair acts or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45, and violate the Gramm-Leach-Bliley Act ("GLB Act"), 15 U.S.C. § 6801.

---

[40] Federal Trade Commission, *Start With Security*, *supra* n 30.

[41] *See* Federal Trade Commission, *Privacy and Security Enforcement Press Releases*, available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Feb. 15, 2022).

E. Defendants Contravene the Purpose of the Driver's Privacy Protection Act

71. Prior to the enactment of the Driver's Privacy Protection Act, Congress found that most states freely turned over DMV information to whomever requested it with only few restrictions. 137 Cong. Rec. 27,327 (1993).

72. Due to this lack of restrictions, Congress grew concerned that potential criminals could easily access home addresses and telephone numbers of potential victims. 140 Cong. Rec. 7929 (1994) (statement of Rep. Porter Goss).

73. These concerns did, in fact, materialize in the occurrence of crime, harassment, and stalking. Most notably, in 1989, a stalker shot and killed Rebecca Schaeffer, an upcoming actor, after obtaining her unlisted home address from the California DMV. 137 Cong. Rec. 27,327 (1993). In advocating for the DPPA, Representative Jim Moran (D-VA) recounted thieves using information from the DMV to learn home addresses and commit burglary and theft. 137 Cong. Rec. 27,327 (1993). Similarly, Senator Barbara Boxer (D-CA) explained how a man used the DMV to obtain the home addresses of several young women and sent them harassing letters. 39 Cong. Rec. 29,466 (1993). In another instance, a woman who visited a clinic that performed abortions found black balloons outside her home after a group of anti-abortion activists sought to harass her upon seeing her car in the clinic's parking lot. 139 Cong. Rec. 29,462 (1993) (statement of Sen. Chuck Robb).

74. In light of public outrage over the Schaeffer murder and growing concern for the threat to public safety that free access to DMV records posed, Congress enacted the

DPPA "to protect the personal privacy and safety of licensed drivers consistent with the legitimate needs of business and government." S. Res. 1589, 103rd Cong. §1(b), 139 Cong. Rec. 26,266 (1993) (enacted).

75. Additionally, in enacting the DPPA, Congress was motivated by its "[c]oncern[] that personal information collected by States in the licensing of motor vehicle drivers was being released – even sold – with resulting loss of privacy for many persons." *Akkawi v. Sadr*, 2:20-CV-01034-MCE-AC, 2021 WL 3912151, at *4 (E.D. Cal. Sept. 1, 2021) (citing *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013) (alterations in original)). The sale of private information like driver's license numbers and other motor vehicle records was the exact impetus for the DPPA's passage.

76. As such, Congress sought to expressly prohibit "disclosing personal information obtained by the department in connection with a motor vehicle record." *Chamber of Commerce of United States v. City of Seattle*, 274 F. Supp. 3d 1140, 1154 (W.D. Wash. 2017). Driver's license numbers are thus explicitly listed as "personal information" from "motor vehicle records" under the DPPA. *See* 18 U.S.C. 2725(1).

77. By making the PI of Plaintiff and the Class publicly available, Defendants ran afoul the purpose of DPPA, and threatened the privacy and safety of licensed drivers, for whose protection the statute was enacted. Defendants' actions constituted a concrete injury and particularized harm to Plaintiff and members of the Class, that would not have happened but for Defendants' failure to follow the DPPA. Plaintiff was harmed by the public disclosure of his private facts in addition to the other harms enumerated herein.

F. Plaintiff's Injuries—Attempts to Secure PI After the Disclosure.

78. Defendants admitted there was unauthorized access to and disclosure of Plaintiff's and Class Members' PI in the Notice letter.[42] In the letter, Defendants also recognized that the unauthorized access and disclosure created imminent harm to Plaintiff and Class Members—and specifically stated it "believe[s] this data could be used to fraudulently apply for unemployment benefits" and tasked Plaintiff and Class Members with reviewing written communications from state unemployment agencies for fraudulently filed applications.[43] Defendants also offered a year of credit monitoring due to the imminent risk to Plaintiff and Class Members.[44] Plaintiff and Class Members have been, and will continue to be, injured because they are now forced to spend time monitoring their credit and governmental communications—per Defendants' instructions, guarding against identity theft, and resolving fraudulent claims and charges because of Defendants' actions and/or inactions.

79. Plaintiff Park received a notice from Defendants dated January 14, 2022 ("Notice Letter"). The Notice Letter informed him of the Unauthorized Data Disclosure, stating it believed an unauthorized party used an automated bot process to obtain his driver's license number, and it believed his improperly disclosed driver's license number could be used to fraudulently apply for unemployment benefits in his name.[45] Plaintiff Park

[42] *See supra* n. 4.
[43] *Id.*
[44] *Id.*
[45] *See supra* n.4.

was not a customer of Defendants and had not requested an insurance quote from Defendant.

80. Following the Unauthorized Data Disclosure in December 2021, and before Defendants provided notice of the Unauthorized Data Disclosure, Plaintiff Park became a victim of identity theft as a result of the Unauthorized Data Disclosure. Plaintiff Park received notice from Wells Fargo Bank dated January 6, 2022, stating someone had completed an online application and unsuccessfully attempted to open an account in his name—likely someone utilizing his PI obtained as part of the Unauthorized Data Disclosure. Plaintiff Park spent time calling Wells Fargo Bank to report the fraudulent attempt to open an account in his name. He spent additional time and effort filing a police report about the incident.

81. Plaintiff Park is aware of a second attempt by someone to commit identity theft and fraud. Plaintiff Park received a letter from JPMorgan Chase Bank, N.A., dated January 17, 2022, stating someone had unsuccessfully applied for a CHASE SAPPHIRE Visa Signature account in his name—again, likely someone utilizing his PI obtained as part of the Unauthorized Data Disclosure. Plaintiff Park spent time calling Chase Bank to report the fraudulent attempt to open an account in his name. He spent additional time and effort filing a police report about the incident. Prior to these two incidents that occurred within two months of the Unauthorized Data Disclosure, Plaintiff Park had never been a victim of attempted identity theft and fraud.

82. Upon receiving notice of the above, and the Notice Letter from Defendants, Plaintiff spent time researching his options to respond to the theft of his driver's license,

and the use of same to commit identity fraud. He spent and continues to spend additional time reviewing his credit and financial documents concerning the security of his identity. This is time Plaintiff Park otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

83. Plaintiff Park is also concerned about hackers obtaining his tax returns. He uses TurboTax software, which requires the filer to input their driver's license number, expiration date and issue date as an added security measure. As a result, of the theft of his driver's license number, he delayed the filing of his tax returns.

84. Additionally, Plaintiff Park has never knowingly transmitted unencrypted PI over the internet or any other unsecured source. He deletes any and all unencrypted, non-password protected electronic documents containing his PI and destroys any documents that contain any of his PI, or that may contain any information that could otherwise be used to compromise his PI. Plaintiff Park has never received a notice that his driver's license number or other PI was compromised in any other data breach or unauthorized data disclosure.

85. Plaintiff Park suffered actual injury from having his PI exposed as a result of the Unauthorized Data Disclosure including, but not limited to: (a) identity fraud; (b) loss of his privacy; and (c) imminent and impending further injury arising from the increased risk of fraud and identity theft.

86. The identity theft suffered by Plaintiff Park is logically and temporally linked to the Unauthorized Data Disclosure in the same way that other data breach cases have found to be "fairly traceable." His driver's license number was stolen shortly before he

experienced two different attempts at opening a credit card in his name – a form of identity theft specifically linked to stolen driver's license numbers.

87. As a result of the Unauthorized Data Disclosure, Plaintiff Park was a victim of identity theft, and will continue to be at heightened risk for financial fraud, future identity theft, other forms of fraud, and the attendant damages, for years to come.

F. Plaintiff and Class Members Suffered Additional Damages.

88. Plaintiff and Class Members are at risk for actual identity theft in addition to all other forms of fraud.

89. The ramifications of Defendants' disclosure and failure to keep individuals' PI secure are long lasting and severe. Once PI is disseminated to unauthorized parties, fraudulent use of that information and damage to victims may continue for years.[46]

90. Plaintiff's and Class Members' PI is private, valuable, and sensitive in nature as it can be used to commit a lot of different harms and fraud in the hands of the wrong people. Defendants failed to obtain Plaintiff's and Class Members' consent to disclose such PI to any other person, as required by applicable law and industry standards.

91. Defendants' inattention to the possibility that anyone, especially thieves with various pieces of individuals' PI, could obtain any individual's PI by utilizing Defendants' front-facing online instant quote platform left Plaintiff and Class Members with no ability to protect their sensitive and private information.

[46] *2014 LexisNexis True Cost of Fraud Study*, (August 2014), *available at*: https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last visited Feb. 15, 2022).

92. Defendants had the resources necessary to prevent the Unauthorized Data Disclosure, but neglected to adequately implement data security measures, despite their obligations to protect Plaintiff's and Class Members' PI from unauthorized disclosure.

93. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, it would have prevented the unauthorized access, disclosure, and ultimately, the theft of PI.

94. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Unauthorized Data Disclosure on their lives.

95. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[47]

96. As a result of Defendants' failure to prevent the Unauthorized Data Disclosure, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft, and/or unauthorized use of their PI,

[47] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last visited Feb. 15, 2022).

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud,

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud,

d. The continued risk to their PI, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the PI in their possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Unauthorized Data Disclosure for the remainder of the lives of Plaintiff and Class Members.

97. In addition to a remedy for the economic harm, Plaintiff and Class Members maintain an undeniable interest in ensuring that their PI is secure, remains secure, and is not subject to further misappropriation and theft.

98. To date, other than providing 12 months of credit monitoring and identity protection services, Defendants do not appear to be taking any measures to assist Plaintiff and Class Members other than simply telling them to do the following:

- "regularly review statements from your accounts"
- "periodically obtain your credit report"
- "remain vigilant with respect to viewing your account statements and credit reports"

- obtain a copy of a free credit report
- contact the FTC and/or the state Attorney General's office to obtain additional information about avoiding identity theft

None of these recommendations, however, require Defendants to expend any effort to protect Plaintiff's and Class Members' PI. It is also not clear that Defendants have made any determination that the credit monitoring and identity protection services are designed or adequate to ameliorate the specific harms of having an exposed driver's license number and address.

99. Defendants' failure to adequately protect Plaintiff's and Class Members' PI has resulted in Plaintiff and Class Members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money. Instead, as Defendants' Notice indicates, they are putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

100. Defendants' offer of 12 months of identity monitoring and identity protection services to Plaintiff and Class Members is woefully inadequate. While some harm has begun already, the worst may be yet to come. There may be a time lag between when additional harm occurs versus when it is discovered, and also between when PI is acquired and when it is used.

CLASS ACTION ALLEGATIONS

101. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and the following proposed Nationwide Class (the "Class") as defined as follows:

> Nationwide Class: All persons in the United States whose PI was compromised in the Unauthorized Data Disclosure announced by Defendants on or near January 14, 2022.

102. Pursuant to Federal Rules of Civil Procedure 23(b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of the following California state subclass ("California Subclass"):

> California Subclass: All persons in California whose PI was compromised in the Unauthorized Data Disclosure announced by Defendants on or near January 14, 2022.

103. The Nationwide Class and California Subclass are collectively referred to herein as "Class" unless otherwise stated.

104. Excluded from the proposed Class are any officer or director of Defendants; any officer or director of any affiliate, parent, or subsidiary of Defendants; anyone employed by counsel in this action; and any judge to whom this case is assigned, his or her spouse, and members of the judge's staff.

105. **Numerosity.** Members of the proposed Class likely number in at least the thousands and are thus too numerous to practically join in a single action. Membership in the Class is readily ascertainable from Defendants' own records.

106. **Commonality and Predominance.** Common questions of law and fact exist as to all proposed Class Members and predominate over questions affecting only individual Class Members. These common questions include:

a. Whether Defendants engaged in the wrongful conduct alleged herein,

b. Whether Defendants' inadequate data security measures were a cause of the Unauthorized Data Disclosure,

c. Whether Defendants knew that its online quoting platforms were capable of improperly disclosing driver's license numbers to unauthorized parties and/or entities;

d. Whether Defendants negligently or recklessly breached legal duties owed to Plaintiff and the other Class Members to exercise due care in collecting, storing, and safeguarding their PI,

e. Whether Defendants' online quote system auto-populated prospective quotes with PI obtained from the records of Defendants or third parties without the permission or consent of Plaintiff and the Class,

f. Whether Plaintiff and the Class are at an increased risk for identity theft because of the data security breach,

g. Whether Defendants violated the Drivers' Privacy Protection Act, 18 U.S.C. § 2724,

h. Whether Plaintiff and the Class Members are entitled to actual, statutory, or other forms of damages, and other monetary relief, and

i. Whether Plaintiff and the Class Members are entitled to equitable relief, including, but not limited to, injunctive relief and restitution.

107. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff individually and on behalf of the other Class Members. Similar or identical statutory and common law violations, business practices,

and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous questions that dominate this action.

108. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Class. All Class Members were subject to the Unauthorized Data Disclosure and had their PI accessed by, used and/or disclosed to unauthorized third parties. Defendants' misconduct impacted all Class Members in the same manner.

109. **Adequacy of Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class Members he seeks to represent; he retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

110. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiff and the Class Members pale compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far

fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

FIRST CAUSE OF ACTION

Violation of the Drivers' Privacy Protection Act ("DPPA"), 18 U.S.C. § 2724
(On behalf of Plaintiff, the Nationwide Class, and California Subclass)

111. Plaintiff incorporates the above allegations by reference.

112. DPPA provides that "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains." 18 U.S.C. § 2724.

113. The DPPA also restricts the resale and redisclosure of personal information, and requires authorized recipients to maintain records of each individual and the permitted purpose of the disclosure for a period of five years. 18 U.S.C. § 2721(c).

114. Under the DPPA, a "'motor vehicle record' means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.'" 18 U.S.C. § 2725(1). Drivers' license numbers are motor vehicle records and personal information under the DPPA. 18 U.S.C. § 2725(3); *see also Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 943 (7th Cir. 2015).

115. American Family obtains, uses, and discloses motor vehicle records from its customers.

116. Defendants also obtain motor vehicle records directly from state agencies or through resellers who sell such records.

117. Defendants knowingly published information to the public on their free online quoting platform, accessible from www.amfam.com.

118. Defendants knowingly linked their respective public websites to systems and/or networks storing, maintaining, and/or obtaining Plaintiff's and Class Members' PI.

119. During the time period up until and including at least December 11, 2021, PI, including drivers' license numbers, of Plaintiff and Class Members, were publicly available and viewable on Defendants' online instant quote platform, and Defendants knowingly used and disclosed and/or redisclosed Plaintiff's and Class Members' motor vehicle records and PI to the general public, which is not an authorized use permitted by the DPPA pursuant to 18 U.S.C. §§ 2724, 2721(b), and 2721(c).

120. As a result of the Unauthorized Data Disclosure, Plaintiff and putative Class Members are entitled to actual damages, liquidated damages, punitive damages, attorneys' fees and costs.

SECOND CAUSE OF ACTION

Negligence
(On behalf of Plaintiff, the Nationwide Class, and California Subclass)

121. Plaintiff incorporates the above allegations by reference.

122. Defendants owed a duty to Plaintiff and the Class Members to exercise reasonable care in obtaining, securing, safeguarding, storing, and protecting Plaintiff's and Class Members' PI from being compromised, lost, stolen, and accessed by unauthorized

persons. This duty includes, among other things, designing, implementing, maintaining, and testing their data security systems to ensure Plaintiff's and Class Members' PI in Defendants' possession, or that could be accessed by Defendants, was adequately secured and protected.

123. Defendants owed a duty of care to Plaintiff and Members of the Class to provide security, consistent with industry standards, to ensure that their systems and networks adequately protected PI it stored, maintained, used, and/or obtained.

124. Defendants owed a duty of care to Plaintiff and Members of the Class because they were foreseeable and probable victims of any inadequate data security practices. Defendants knew or should have known of the inherent risks in having their systems auto-populate online quote requests with private PI without the consent or authorization of the person whose PI was being provided.

125. Unbeknownst to Plaintiff and Class Members, they were entrusting Defendants with their PI when Defendants obtained their PI from motor vehicle records directly from state agencies or through resellers who sell such records. Defendants had an obligation to safeguard Plaintiff's and Class Members' information and was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Unauthorized Data Disclosure.

126. Defendants' own conduct also created a foreseeable risk of harm to Plaintiff and Class Members and their PI. Defendants' misconduct included failing to implement the systems, policies, and procedures necessary to prevent the Unauthorized Data Disclosure.

127. Defendants acknowledge their conduct created actual harm to Plaintiff and Class Members because Defendants warned of potential fraudulent unemployment benefits claims in their names as a result of the Unauthorized Data Disclosure, and offered one year of credit monitoring.

128. Defendants knew, or should have known, of the risks inherent in collecting and storing PI and the importance of adequate security. Defendants knew about—or should have been aware of—numerous, well-publicized unauthorized data disclosures affecting businesses, especially insurance and financial businesses, in the United States.

129. Defendants breached their duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security to safeguard Plaintiff's and Class Members' PI.

130. Because Defendants knew that a breach of their systems would damage thousands of individuals whose PI was inexplicably stored or was accessible, including Plaintiff and Class Members, Defendants had a duty to adequately protect their data systems and the PI contained and/or accessible therein.

131. Defendants also had independent duties under state and federal laws requiring Defendants to reasonably safeguard Plaintiff's and Class Members' PI.

132. In engaging in the negligent acts and omissions as alleged herein, which permitted thieves to access Defendants' systems that stored and/or had access to Plaintiff's and Class Members' PI, Defendants violated Section 5 of the FTC Act, which prohibits "unfair…practices in or affecting commerce," and the GLB Act. This includes failing to

have adequate data security measures and failing to protect Plaintiff's and the Class Members' PI.

133. Plaintiff and the Class Members are among the class of persons Section 5 of the FTC and the GLB Act were designed to protect, and the injuries suffered by Plaintiff and Class Members are the types of injury Section 5 of the FTC Act and the GLB Act were intended to prevent.

134. Neither Plaintiff nor the other Class Members contributed to the Unauthorized Data Disclosure as described in this Complaint.

135. As a direct and proximate cause of Defendants' conduct, Plaintiff and Class Members have suffered and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their PI is used; (ii) the publication and/or theft of their PI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Unauthorized Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest and recover from unemployment and/or tax fraud and identity theft; (v) costs associated with placing freezes on credit reports; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PI, which remains in Defendants' possession (and/or Defendants had access to) and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PI in their continued possession; and, (viii) future costs

in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PI.

THIRD CAUSE OF ACTION

Violation of the California Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq*.
(Brought by Plaintiff and the California Subclass)

136. Plaintiff incorporates the above allegations by reference.

137. Plaintiff and the California Subclass members are "consumer[s]" as that term is defined in Cal. Civ. Code § 1798.140(g).

138. American Family is a "business" as that term is defined in Cal. Civ. Code. § 1798.140(c). American Family collects consumers' (including Plaintiff's and California Subclass Members') personal information and determines the purposes and means of the processing of this personal information (e.g., it collects PI for the purpose of analyzing the information for insurance quotes, and designs the systems that process and store consumers' PI). American Family annually receives for commercial purposes or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers.

139. Plaintiff and California Subclass Members' PI is "nonencrypted and nonredacted personal information" as that term is used in Cal. Civ. Code § 1798.150(a)(1). At a minimum, this PI included the individual's name and unique identification number issued on government documents (e.g., driver's license number).

140. The Unauthorized Data Disclosure constitutes "an unauthorized access and exfiltration, theft, or disclosure" pursuant to Cal. Civ. Code § 1798.150(a)(1).

141. Under the CCPA, American Family had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the Plaintiff's and California Subclass Members' PI to protect said PI.

142. American Family breached the duty it owed to Plaintiff and California Subclass Members by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect Plaintiff's and California Subclass Members' PI; (b) detect the Data Breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

143. Defendants' breach of the duty it owed to Plaintiff and California Subclass Members described above was the direct and proximate cause of the Data Breach. As a result, Plaintiff and California Subclass members suffered damages, as described above and as will be proven at trial.

144. Plaintiff seeks injunctive relief in the form of an order enjoining Defendants from continuing the practices that constituted their breach of the duty owed to Plaintiff and California Subclass Members as described above, and to implement improved security procedures and measures, specifically:

a. Ordering Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors,

b. Ordering Defendants engage third–party security auditors and internal personnel to run automated security monitoring,

c. Ordering American Family audit, test, and train its security personnel regarding any new or modified procedures,

d. Ordering Defendants not to make PI available on their instant quote webpage,

e. Ordering Defendants not to store PI or make PI accessible in any publicly facing website,

f. Ordering Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services,

g. Ordering Defendants conduct regular computer system scanning and security checks; and

h. Ordering Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a breach.

145. Plaintiff also seeks actual damages, and all other forms of relief available under the CCPA.

146. Contemporaneously with filing this Complaint, and on or about March 28, 2022, Plaintiff sent via registered mail the 30-day notice letter as required under Civil Code section 1798.150, subd. (b). Plaintiff and California Subclass Members reserve the right to amend this Complaint as of right to seek statutory damages and relief following the expiration of the 30-day period.

FOURTH CAUSE OF ACTION

Violation of the California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On behalf of Plaintiff, the Nationwide Class, and California Subclass)

147. Plaintiff incorporates the above allegations by reference.

148. By reason of the conduct alleged herein, American Family engaged in unlawful and unfair business practices within the meaning of California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

149. American Family stored, disclosed, and/or provided access to Plaintiff's and Class Members' PI through its online quote platform.

150. Defendants knew or should have known it did not employ reasonable, industry standard, and appropriate security measures in compliance with federal regulations that would have kept Plaintiff's and Class Members' PI secure, and prevented the unauthorized disclosure, loss, or misuse of that PI.

Unlawful Business Practices.

151. Defendants violated the DPPA, Section 5(a) of the FTC Act, the GLB Act, and California Civil Code § 1798.81.5(b) by failing to implement and maintain reasonable and appropriate security measures or follow industry standards for data security.

152. If Defendants had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Unauthorized Data Disclosure.

153. Plaintiff and Class Members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In addition, Plaintiff's

and Class Members' PI was accessed, disclosed, taken, viewed, and now in the possession of those who will use it for their own advantage, and/or is being sold for value—making it clear that Plaintiff's and Class Members' PI is of tangible value. Plaintiff and Class Members have also suffered consequential out-of-pocket losses for procuring credit freezes, credit protection services, identity theft monitoring, and/or other expenses relating to identity theft losses or protective measures.

Unfair Business Practices.

154. Balancing Test. Defendants engaged in unfair business practices under the "balancing test." The harm caused by Defendants' actions and omissions, as described in detail above, greatly outweigh any perceived utility. Indeed, none of Defendants' actions or inactions can be said to have had any utility at all. Defendants' failures were clearly injurious to Plaintiff and Class Members, directly causing the harms alleged in the Complaint.

155. Tethering Test. Defendants also engaged in unfair business practices under the "tethering test." Defendants' actions and omissions, as described in detail above, violated fundamental public policies expressed by the California Legislature. (*See, e.g.*, Cal. Civ. Code § 1798.1, "The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."; Cal. Civ. Code § 1798.81.5(a), "It is the intent of the Legislature to ensure that personal information about California residents is protected."; Cal. Bus. & Prof. Code § 22578, "It is the intent of the Legislature that this chapter

[including the Online Privacy Protection Act] is a matter of statewide concern.") Therefore, Defendants' acts and omissions amount to a violation of the law.

156. FTC Test. Defendants engaged in unfair business practices under the "FTC test." The harm caused by Defendants' actions and omissions, as described in detail above, are substantial in that they affect Plaintiff and thousands of Class Members, and caused them to suffer actual harms. Such harms include actual identity theft, a substantial and continuing risk of identity theft, disclosure of Plaintiff's and Class Members' PI to third parties without their consent, diminution in value of their PI, consequential out-of-pocket losses for procuring credit freezes, credit protection services, identity theft monitoring, and/or other expenses relating to identity theft losses or protective measures. This harm continues for two reasons. First, Plaintiff's and Class Members' PI remains in Defendants' possession, without adequate protection. Second, Plaintiff's and Class Members' PI is now possessed by those who obtained it without Plaintiff's and Class Members' consent. Defendants' actions and omissions violated Section 5(a) of the Federal Trade Commission Act. (*See* 15 U.S.C. § 45(n), defining "unfair acts or practices" as those that "cause[ ] or [are] likely to cause substantial injury to consumers which [are] not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition"; *see also, e.g.*, *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016), failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act).

157. Plaintiff and Class Members suffered injury in fact, and lost money or property as the result of Defendants' unfair business practices. Plaintiff's and Class

Members' PI was improperly accessed, disclosed, and taken and is now in the hands of those who will use it for their own advantage, potentially—and likely—selling the PI for value—making it clear that Plaintiff's and Class Members' PI is of tangible value. Plaintiff and Class Members have also suffered consequential out-of-pocket losses for procuring credit freezes, credit protection services, identity theft monitoring, and/or other expenses relating to identity theft losses or protective measures.

158. As a result of Defendants' unlawful and unfair business practices in violation of the UCL, Plaintiff and Class Members are entitled to equitable and injunctive relief, including restitution or disgorgement.

FIFTH CAUSE OF ACTION

Declaratory and Injunctive Relief
(On behalf of Plaintiff, the Nationwide Class, and California Subclass)

159. Plaintiff incorporates the above allegations by reference.

160. This Count is brought under the federal Declaratory Judgment Act, 28 U.S.C. § 2201.

161. As previously alleged, Plaintiff and Class Members had a reasonable expectation that companies such as Defendant, who could access their PI through automated systems, would provide adequate security for that PI.

162. American Family owes a duty of care to Plaintiff and Class Members requiring it to adequately secure PI.

163. Defendants still possess PI regarding Plaintiff and Class Members.

164. Since the Unauthorized Data Disclosure, Defendants announced few if any changes to their data security infrastructure, processes, or procedures to fix the vulnerabilities in their computer systems and/or security practices which permitted the Unauthorized Data Disclosure to occur and, thereby, prevent further attacks. This is true despite the fact that Defendants have suffered the exact same Unauthorized Data Disclosure multiple times.

165. The Unauthorized Data Disclosure caused actual harm because of Defendants' failure to fulfill their duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PI and Defendants' failure to address the security failings that lead to such exposure.

166. There is no reason to believe that Defendants' security measures are more adequate now than they were before the Unauthorized Data Disclosure to meet Defendants' legal duties.

167. Plaintiff, therefore, seeks a declaration (1) that Defendants' existing security measures do not comply with their duties of care to provide adequate security, and (2) that to comply with their duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis,

and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors,

b. Ordering Defendants engage third–party security auditors and internal personnel to run automated security monitoring,

c. Ordering American Family audit, test, and train its security personnel regarding any new or modified procedures,

d. Ordering Defendants not to make PI available on their instant quote webpage,

e. Ordering Defendants not to store PI or make PI accessible in any publicly facing website,

f. Ordering Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services,

g. Ordering Defendants conduct regular computer system scanning and security checks; and

h. Ordering Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a disclosure when it occurs and what to do in response to a breach.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all others similarly situated, respectfully requests the Court enter an order:

a. Certifying the proposed Class as requested herein,

b. Appointing Plaintiff as Class Representative and undersigned counsel as Class Counsel,

c. Finding that Defendants engaged in the unlawful conduct as alleged herein,

d. Granting injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein,

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws,

iii. requiring Defendants to delete, destroy, and purge the personal information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members,

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' personal information,

v. prohibiting Defendants from maintaining Plaintiff's and Class Members' personal information on any cloud-based database,

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to

conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors,

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring,

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures,

ix. requiring Defendants to conduct regular database scanning and security checks,

x. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal information, as well as protecting the personal information of Plaintiff and Class Members,

xi. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,

xii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed

in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal information,

xiii. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,

xiv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal information to third parties, as well as the steps affected individuals must take to protect themselves,

xv. requiring Defendants to design, maintain, and test their computer systems to ensure that PI in their possession is adequately secured and protected,

xvi. requiring Defendants disclose any future data disclosures in a timely and accurate manner, including its previous data disclosures and failures; and

xvii. requiring Defendants to provide ongoing credit monitoring and identity theft repair services to Class Members.

e. Awarding Plaintiff and Class Members damages,

f. Awarding Plaintiff and Class Members pre-judgment and post-judgment interest on all amounts awarded,

g. Awarding Plaintiff and the Class Members reasonable attorneys' fees, costs, and expenses; and

h. Granting such other relief as the Court deems just and proper.

VI. DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the proposed Class, hereby demands a trial by jury as to all matters so triable.

Dated: March 28, 2022

/s/ David W. Asp

David W. Asp (MN #344850)
Kate M. Baxter-Kauf (MN #0392037)
Karen Hanson Riebel (MN #0219770)
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
dwasp@locklaw.com
kmbaxter-kauf@locklaw.com
khriebel@locklaw.com

GAYLE M. BLATT
CASEY GERRY SCHENK FRANCAVILLA BLATT & PENFIELD, LLP
Gayle M. Blatt
P. Camille Guerra
110 Laurel Street
San Diego, CA 92101
Telephone: (619) 238-1811
Facsimile: (619) 544-9232
gmb@cglaw.com
camille@cglaw.com

Attorneys for Plaintiff and the putative Class